Claims

What is claimed is:

1. A method for encrypting a message to be transmitted over a network, wherein the method comprises the steps of:

encrypting the message for transmission over the network, the resulting encrypted message having associated therewith a proof of correctness indicating that the message is of a type that allows decryption by one or more escrow authorities; and

transmitting the encrypted message through the network to a recipient, wherein in traversing the network the proof of correctness associated with the encrypted message is checked by at least one module of a server of the network.

2. The method of claim 1 wherein the encrypted message is generated by first selecting a random element k from an interval $[0 \ldots q\text{-}1]$, where q denotes the size of a group G, using modulo p, then computing a symmetric key $K = \text{hash}(g^k \bmod p)$ for a symmetric encryption technique (E, D), where g is a generator of the group G, and finally computing the encrypted message in the form of a ciphertext $M' = E_K(M)$, where M denotes the message being encrypted.

3. The method of claim 1 wherein also associated with the encrypted message is an element $a = y_d^{\alpha} * g^k$ and an element $b = g^{\alpha}$, where α is chosen uniformly at random from $[0 \ldots q\text{-}1]$ and y_d is a public encryption key.

4. The method of claim 3 wherein the proof of correctness comprises a proof of knowledge of (α, k) that does not reveal y_d^{α} or g^k.

5. The method of claim 1 wherein also associated with the encrypted message is a certificate C_d on a public encryption key y_d.

6. The method of claim 5 wherein the encrypted message is considered valid by the module of the server if the proof of correctness is valid and the certificate C_d is valid.

7. The method of claim 6 wherein the certificate C_d is considered valid if it is a valid certificate for encryption.

8. The method of claim 1 wherein the proof of correctness comprises a proof c in the form of a triple (r, $s1$, $s2$).

9. The method of claim 8 wherein the proof c is generated using the steps of:

selecting two elements $\beta 1$ and $\beta 2$ at random from an interval $[0 \ldots q\text{-}1]$;

computing $r = y_d^{\beta 2} g^{\beta 2} \pmod p$;

computing $e = \text{hash}(r, a)$;

computing $s1 = \beta 1 + e * \alpha \pmod q$;

computing $s2 = \beta 2 + e * k \pmod q$; and

outputting the triple (r, $s1$, $s2$) as the proof c.

10. The method of claim 2 wherein the encrypted message is decrypted by a recipient using the steps of:

computing $B = b^{x_d} \pmod p$, where x_d is a secret key corresponding to a public key y_d;

computing $K = \text{hash}(a/B \bmod p)$; and

computing the message M as $M = D_K(M')$.

11. The method of claim 8 wherein the proof of correctness comprising the proof c in the form of the triple (r, $s1$, $s2$) is checked by computing $e = \text{hash}(r, a)$ and verifying that $y_d^{s1} * g^{s2} = r * a^e$.

12. The method of claim 1 wherein if the check of the proof of correctness indicates that the proof is invalid, the module of the server directs that the encrypted message be discarded.

13. The method of claim 1 wherein the network comprises a plurality of servers, and wherein each of at least a subset of the servers includes a module for checking the proof of correctness if the corresponding encrypted message passes through the corresponding server in being transmitted from a sender to the recipient through the network.

14. The method of claim 1 wherein the one or more escrow authorities comprises an escrow authority associated with a public key used for encryption of the message, and wherein the escrow authority associated with the public key is able to decrypt the encrypted message to obtain a plaintext message.

15. The method of claim 14 wherein the escrow agent associated with the public key is able to decrypt the encrypted message without exposing a corresponding secret key, using a threshold-based method.

16. The method of claim 1 wherein associated with the encrypted message is a first element that is generated using a public key of the recipient and can be decrypted by a party holding the corresponding secret key, and a second element that proves that the first element can be decrypted by a party holding the corresponding secret key.

17. An apparatus for encrypting a message to be transmitted over a network, wherein the apparatus comprises:

a processor-based device for encrypting the message for transmission over the network, the resulting encrypted message having associated therewith a proof of correctness indicating that the message is of a type that allows decryption by one or more escrow authorities; wherein the encrypted message is transmitted through the network to a recipient, and in traversing the network the proof of correctness associated with the encrypted message is checked by at least one module of a server of the network.

18. An article of manufacture comprising one or more software programs for use in encrypting a message to be transmitted over a network, wherein the one or more software programs when executed implement the step of:

encrypting the message for transmission over the network, the resulting encrypted message having associated therewith a proof of correctness indicating that the message is of a type that allows decryption by one or more escrow authorities;

wherein the encrypted message is transmitted through the network to a recipient, and wherein in traversing the network the proof of correctness associated with the encrypted message is checked by at least one module of a server of the network.